Received 5 March 2021
Revised 15 June 2021
Accepted 17 June 2021

A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs

Karen Renaud
University of Strathclyde, Glasgow, UK;
Rhodes University, Grahamstown, South Africa;
University of South Africa, Pretoria, South Africa and
Abertay University, Dundee, UK, and
Jacques Ophoff
Abertay University, Dundee, UK and
University of Cape Town, Cape Town, South Africa

Abstract

Purpose – There is widespread concern about the fact that small- and medium-sized enterprises (SMEs) seem to be particularly vulnerable to cyberattacks. This is perhaps because smaller businesses lack sufficient situational awareness to make informed decisions in this space, or because they lack the resources to implement security controls and precautions.

Design/methodology/approach – In this paper, Endsley's theory of situation awareness was extended to propose a model of SMEs' cyber situational awareness, and the extent to which this awareness triggers the implementation of cyber security measures. Empirical data were collected through an online survey of 361 UK-based SMEs; subsequently, the authors used partial least squares modeling to validate the model.

Findings – The results show that heightened situational awareness, as well as resource availability, significantly affects SMEs' implementation of cyber precautions and controls.

Research limitations/implications – While resource limitations are undoubtedly a problem for SMEs, their lack of cyber situational awareness seems to be the area requiring most attention.

Practical implications – The findings of this study are reported and recommendations were made that can help to improve situational awareness, which will have the effect of encouraging the implementation of cyber security measures.

Originality/value – This is the first study to apply the situational awareness theory to understand why SMEs do not implement cyber security best practice measures.

Keywords SME, Situational awareness, Cyber security precautions and controls

Paper type Research paper

1. Introduction

Small- and medium-sized enterprises (SMEs), businesses with fewer than 250 employees (Ward, 2021), represent the majority of businesses worldwide and play an important role in economic development. Within the United Kingdom (UK), SMEs account for 99.9% of the business population, with the majority (99.3%) having fewer than 50 employees

Organizational Cybersecurity Journal: Practice, Process and People
Vol. 1 No. 1, 2021
pp. 24-46
Emerald Publishing Limited
e-ISSN: 2635-0289
p-ISSN: 2635-0270
DOI 10.1108/OCJ-03-2021-0004

We thank the Scottish Government for funding this research and Keith McDevitt for sponsoring this research.

(UK Department for Business, Energy and Industrial Strategy, n.d.). It is important for SMEs to take account of cyber security so as to resist cyberattacks and assure resilience if attacks *do* occur. SMEs are not lesser targets: there are indications that they are under constant attack from cyber criminals (Lewis, 2020).

There are signs that SMEs' awareness of the cyber security domain is improving, as highlighted in 2009 (Sharma *et al.*, 2009) and again in 2020 (Whitehead, 2020). This could be attributed to more focused cyber security awareness campaigns targeting SMEs. For example, in the UK, the Government-backed Cyber Essentials scheme provides advice and certification, which requires the implementation of a baseline of technical controls that can help to protect businesses from cyberattacks (CyberEssentials, 2021). The related Cyber Aware campaign provides sole traders and small businesses with a bespoke action plan to improve their cyber security (CyberAware, 2021).

Even so, it must be acknowledged that other parts of the world do not benefit from the same kinds of government-sponsored SME-specific awareness drives (Lejaka *et al.*, 2019). Research also shows that SMEs remain vulnerable because they often do not take action to protect their devices and information (Shred-it, 2011; Bell, 2017; Reuter, 2015; Berry and Berry, 2018; Ncubukezi *et al.*, 2020; Renaud and Weir, 2016). SMEs run the risk of falling victim to an attack if they neglect cyber security (Muncaster, 2020; SMESEC, 2021).

With a basic awareness of cyber security becoming less of an issue, the inaction might be due to a lack of situational awareness. In particular, SMEs might not realize that cyber security threats are a very real threat to *them* and that an attack could put them out of business. On the other hand, they might not know which precautions to take or controls to implement. Finally, they might not feel compelled to act on their knowledge to ameliorate the cyber threat. Research in this field is limited by a paucity of empirical data. Our review of prior literature from 2010 onwards (see Section 2) revealed only 18 studies that reported findings based on data collected from *actual* SMEs. This means that we do not have a good understanding of why a wide range of SMEs fail to implement cyber security measures.

In this paper, we use Endsley's model of situational awareness as a lens to examine the reasons for SMEs' perceived failure to implement sufficient cyber security controls and precautions. The research question to be addressed in this paper is: *How do SMEs' cyber situational awareness influence their implementation of cyber security controls and precautions?* We report on a study we carried out with 361 UK-based businesses to investigate this question. The study was conducted using an online survey and, aligned with our focus on SMEs, only included businesses with fewer than 250 employees (Ward, 2021).

The rest of this paper is structured as follows. Section 2 reports on a literature review of cyber security research related to SMEs. Section 3 introduces Endsley's situational awareness model and describes our survey methodology. Thereafter, Section 4 presents our data analysis and findings. Section 5 discusses the implications of our study, its limitations and then concludes.

2. Related research

We commenced by carrying out a systematic review of the academic literature dealing with this topic. The following search terms were used: allintitle: (small OR medium OR midsize OR micro) AND (business OR enterprise OR firm OR company OR organization OR organisation AND security) OR (SME AND security). The search was limited to peer-reviewed English-language papers from 2010 to present. Table 1 shows which databases we searched for relevant papers, as well as the number of papers we found.

The search identified 170 articles matching our search terms (hits). After reviewing all the initial hits and eliminating irrelevant articles, 90 remained. Within this set, 33 duplicate articles were removed and three were unobtainable. A final total of 54 relevant articles

Database	Hits	Reviewed
Academic Search Premier (EBSCO host)	16	11
ABI/INFORM (ProQuest)	44	30
Scopus	60	28
JSTOR	3	3
Web of Science	30	15
ACM Digital Library	0	0
IEEE Xplore	15	1
PsycInfo	2	2
Google Scholar	107	0
Subtotal	170	90
		−36*
Final Total		54

Note(s): *Duplicates and Unobtainable

Table 1. Literature databases searched

remained to support analysis. We supplemented the results from the literature search with government and professional association surveys and guidelines, which focused on cyber security and SMEs. This included relevant industry and government documents published in the UK, EU and USA.

2.1 Metaview of publications

The wider cyber security industry is often focused on larger organizations, and SMEs sometimes attempt to follow their recommendations, such as ensuring that they have security policies (Kimwele *et al.*, 2010; González *et al.*, 2013; Almeida *et al.*, 2018). Policies, in and of themselves, are but one component of a comprehensive cyber security approach, including a range of technical measures, processes, employee training and information security governance. Many SMEs, especially micro businesses, will find this infeasible. Many SMEs cope by outsourcing information security and use the cloud to ensure information availability (CsC and Stehílková, 2011; Hutchings *et al.*, 2013). However, not all can afford this option.

The research literature covering SMEs and cyber security does offer SME-specific information security guidelines (Sangani and Vijayakumar, 2012; Todd and Rahman, 2015; Harris and Patten, 2014; Brodin and Rose, 2020; Pagura, 2020; Schneider, 2013; Kaušpadienė *et al.*, 2019). However, while these guidelines are excellent, it is also the case that SMEs are not necessarily going to delve into the academic research literature to find the right advice. In the UK, the Federation for Small Businesses [1] does a great job of disseminating valuable cyber security advice, but members pay an annual membership fee, which might be difficult for small businesses, especially in the current climate.

Other researchers suggest SME-specific information security maturity models (Cholez and Girard, 2014; Noguerol and Branch, 2018; Yigit Ozkan *et al.*, 2020) but, once again, this is unlikely to reach the SMEs and maturity models suggest an existing commitment from SMEs whereas the evidence for this level of engagement is not compelling.

2.2 Context-related aspects

The rest of the papers from the literature review suggest a number of deficiencies that could prevent SMEs from implementing cyber security controls and precautions. These fall naturally into three categories: (1) SMEs not understanding the importance of cyber security to their business continuity, (2) a lack of cyber situational awareness and (3) a lack of resources that they need to implement cyber security precautions and controls. Figure 1 depicts the three areas, with each enumerated aspect being dealt with below in more detail.

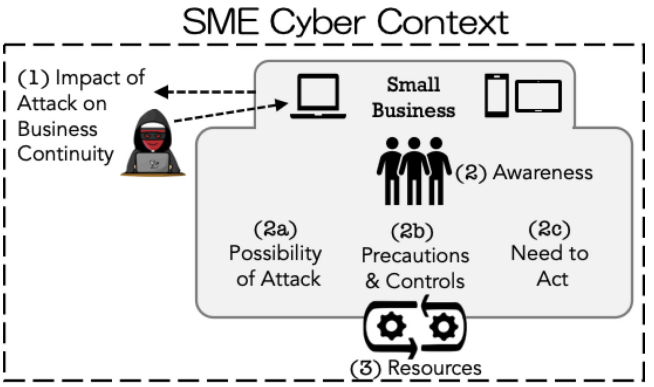


Figure 1. Awareness requirements in the SME cyber context

(1) Not understanding the importance of cyber security to business continuity

SMEs might not appreciate the relevance of cyber security to the long-term health and continuity of their business (Barlette *et al.*, 2017; Mitrofan *et al.*, 2020; Imsand *et al.*, 2019). In reality, 60% of small businesses will close within six months of being hacked (Robert Johnson, 2019). If SME owners think that cannot really hurt their business, they are suffering from a lack of situational awareness.

(2) Awareness

There are three kinds of potential deficits in this area. The first is not realizing that they are vulnerable to attack (2a). If this deficiency is addressed, the second is that there could be a lack of awareness of the precautions that should be taken and controls to be implemented (2b). If this deficiency is addressed, there could still be a lack of awareness of the need to act and to keep up with the latest developments in both threats and measures to be taken (2c).

(2a) Awareness of the Cyber Security Threat Domain

There are failures that are related to SME owners and/or employees not perceiving the reality of the cyber threat reality (Perez, 2020; Sangster, 2020). The 2021 Cyber Breaches survey (Department for Digital, Culture, Media and Sport, 2021) reported that 38% of businesses experienced data breaches in 2021, with the average cost of a breach being £8170. 27% of small businesses are being attacked at least once a week. There is evidence that small businesses are not aware of this situation, given that only 15% have done a cyber security audit (Department for Digital, Culture, Media and Sport, 2021).

(2b) Awareness of Cyber Security Precautions and Controls

SMEs who *are* aware of the reality of the threats and the probability of being attacked will need to know which precautions to take and which controls to implement.

The UK government, probably realizing that a lack of cyber security-related knowledge is a problem, has engaged in a number of endeavors to help improve perceptions. In particular, the Cyber Essentials scheme is worth mentioning. The UK's National Cyber Security Centre (NCSC) introduces the Cyber Essentials scheme (CyberEssentials, 2021) as: "*Cyber Essentials is a simple but effective, Government backed scheme that will help you to protect your organization, whatever its size, against a whole range of the most common cyber attacks.*" To be accredited, organizations need to implement just five controls: (1) Use a firewall, (2) Choose the most secure settings for devices and software, (3) Control access to data and services, (4) Use antivirus software and (5) Install software updates.

UK businesses of all sizes can get Cyber Essentials certification, and there are government sponsored schemes that will give small businesses grants to help them to pay for such certification [2]. Information published by Statista [3] shows that less than a quarter of small businesses in the UK are aware of the scheme.

There is an unwritten assumption that SMEs will seek out advice related to precautions to be taken from reliable sources. The poor uptake of the Cyber Essentials scheme in the UK, as well as various research publications, suggest that this assumption is likely to be naïve (Shred-it, 2011; Reuter, 2015; Berry and Berry, 2018).

Why do SMEs not benefit from freely available guidance? Heidt *et al.*, 2019 and Lacey and James (2010) also report on the **lack of time** SMEs have to really get a handle on all the latest cyber security threats and recommendations.

Lloyd (2020) argues that too many cyber security messages point to cyber security risks and consequences of attacks without highlighting the benefits of implementing cyber security controls and precautions. If fear is used in these messages, people might well end up **avoiding** engaging with cyber security topics altogether (Renaud and Dupuis, 2019; Manheim, 2014; Persoskie *et al.*, 2014)

(2c) Awareness of need to Act on Awareness

Sangster (2020) highlights the fact that many small businesses suffer from misperceptions. For example, they think that they are **too small** or **insignificant** to be targeted by cyber criminals (Nachreiner, 2012; Lacey and James, 2010; Kabanda *et al.*, 2018; Chung, 2020). They may also believe that, given that they have not yet experienced at attack, their current *status quo* cyber security measures are "good enough" (BullGuard, 2020), the so-called **halo effect**.

Multi-dimensionality of controls: SMEs might use these as rationalizations for not implementing cyber security controls (Njenga and Jordaan, 2016). Lacey and James (2010) also refer to a perception that cyber security is a technical issue and not something for business people to be concerned about. This is confirmed by ENISA (2015). These beliefs are clearly misperceptions, preventing SMEs from fully comprehending the situation. Berry and Berry (2018) found that while the small business owners they interviewed often had the technological security tools, they often did not have the policies, procedures and training in place to ensure that their employees knew how to behave securely. This is also emphasized by Kurpjuhn (2015). This leads to a failure factor related to the role of employees in this domain. Employee actions can indeed compromise SMEs' cyber security initiatives (Gundu, 2019). Yet, they can also be an important part of the SMEs' cyber security defense perimeter. Patterson (2017) reported a lack of employee involvement getting in the way of good cyber hygiene in small businesses.

(3) Lack of resources

This kind of failure is related to an SME being aware of the threat, and knowing which actions to take, but not having sufficient resources (Kent *et al.*, 2016). There are number of resources that could be lacking, as suggested by Lee *et al.*, (2019). For example, they might lack ***social resources***, i.e. pressure from their suppliers, customers or competitors (Barlette and Jaouen, 2019) to implement cyber security controls. Also, SMEs might not realize that their employees should be supporting each other. Finally, they might not know that they can obtain security advice from other small businesses who are geographically close to them (Marett and Barnett, 2019).

The next kind of resource is ***organizational.*** SMEs might lack financial resources (Heidt *et al.*, 2019) or experience difficulties prioritizing advice (Redmiles *et al.*, 2020). They might also suffer from information overload (Cenfetelli and Schwarz, 2011; Renaud and Weir, 2016; Gafni and Pavel, 2019) because they do not know which advice to follow.

Finally, they might lack ***personal resources***. For example, Williams (2020), in reporting on the results of the UK government's cyber security survey (Department for Digital, Culture, Media and Sport, 2019), reports that 48% of UK businesses "*lacked the confidence to carry out the kinds of basic tasks laid out*" in the Cyber Essentials scheme. This might lead to *a lack of self-efficacy* (Lent *et al.*, 2006; Vance *et al.*, 2012; Ifinedo, 2012).

3. Situational awareness theory

Endsley (1985) proposed a theory of *situational awareness*, which she defines as "*the perception of the elements of the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future*" (p. 32). According to Endsley, there are three levels of situational awareness.

Level 1: *Being aware of the relevant information about a particular domain*. Such information may come to the person accidently, but often the decision maker will need to seek it out deliberately. This failure aligns well with SMEs being unaware of the reality of the cyber threat, and the very real probability that they could experience a data breach (2a).

Level 2: *Constructing a coherent and comprehensive metaview of the situation.* Merely being aware of the threats will not guarantee that the person will achieve this level. What is required is an understanding of the *import* of knowledge of the threat so that they can make sense of it. Hence, information + comprehension = a nuanced understanding of a situation. This level aligns with SMEs knowing which precautions to take and controls to implement (2b).

Level 3: *Having reached level 2, level 3 is the next stage, during which the person can choose to take action to address the situation, or not*. In deciding to take action, the decision maker will be informed by their own preconceptions. Endsley warns that when preconceptions are accurate, they will lead to correct decisions. On the other hand, they might also be misinformed, and these misperceptions will hamper the person's ability to make the right decision. Even if the person does make a decision to act, they might not have the resources to do so. This final level aligns with inaction due to a lack of resources or information overload (2c).

Endsley (1995) enumerates three specific types of situational awareness errors linked to the three levels mentioned above. The literature review suggests that SMEs could be suffering from a lack of situational awareness, and that this would explain the situation we are observing with respect to SMEs not implementing the controls and precautions that could protect their devices and information.

We now propose an extension of Endsley's situational awareness model to depict an SME cyber situational awareness. Based on the factors identified in this literature review, Figure 2 depicts the proposed SME cyber security situational awareness model. Not understanding that maintaining cyber security is relevant to their business continuity is captured within the "importance of cyber security" construct. The lack of cyber situational awareness is reflected in the center of the model, and the role of a lack of the different kinds of resources feed into cyber situational awareness (social resources) or directly into the implementation of cyber controls and precautions (organizational and personal resources). Table 2 enumerates the hypotheses to be tested to validate this model.

3.1 Methodology

To test our hypotheses, we followed a quantitative methodology using a survey approach. Based on insights gained from the literature review, we designed a questionnaire to gather data within the following categories, as outlined in Table 3.

We validated the questionnaire with a panel consisting of industry professionals working in security roles and academic staff knowledgeable in the area. The panel was asked to

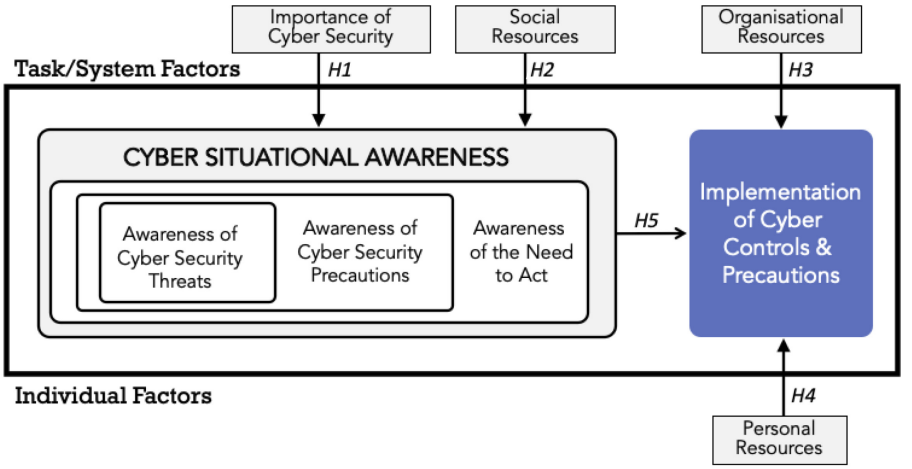


Figure 2.
Proposed SME cyber security situational awareness in decision making model

Note(s): Grounded in Endsley's situational awareness theory (Endsley, 1995)

H1	The SME's understanding of the importance of cyber security influences their cyber situational awareness
H2	The SME's social resources influence their cyber situational awareness
H3	The SME's organizational resources influence the cyber security controls and precautions they implement
H4	The SME's personal resources influence the cyber security controls and precautions they implement
H5	The SME's cyber situational awareness influences the cyber security controls and precautions they implement

Table 2.
Hypotheses to be tested

comment on the completeness and relevance of items, as well as any other issues they identified. After amending the questionnaire to incorporate panel feedback, we conducted a further pilot to validate the survey logic. We only proceeded to collect data after institutional ethical approval for the survey was granted by Abertay University.

We employed a leading online survey platform to collect data using double-opt-in market research panels. Our sampling approach pre-targeted employees in, or owners of, UK-based SMEs. The incidence rate after pre-targeting was at 67%. To ensure data quality, we employed multiple attention checks (180 responses were removed for failing these) and each respondent could only complete the survey once. A total of 361 valid responses were collected during October and November 2020.

4. Data analysis and findings

Prior to analysis, the data were cleaned by removing incomplete answers, or cases with failed attention checks, and certain questions being reverse coded to support analysis. Once the data had been cleaned, we used IBM SPSS Statistics (version 26) to conduct the analysis.

4.1 Business characteristics

About 50% of respondents represented micro businesses (fewer than ten employees), while small and medium businesses consisted of 25% each. A large percentage of responses were

Construct	Questions
(1) Importance of Cyber Security	*Imp1.* How high or low a priority is cyber security to your business? (Very high – Very low) *Imp2.* A tally of the number of risk management arrangements they have in place, as well as the actions taken in the previous year to identify cyber security risks to the business Questions derived from the literature review
(2) Cyber Situational Awareness	*CSA1.* How useful, if at all, is the cyber security information, advice or guidance from Government? (Very useful – Not at all useful/Unaware) *CSA2.* A tally of the Government schemes, information and guidance on cyber security they have heard of *CSA3.* A tally of the number of attacks experienced over the last year *CSA4.* My business is too small for hackers to bother with me (Strongly agree – Strongly disagree) Questions derived from literature review and from (Department for Digital, Culture, Media and Sport, 2019)
(3) Social Resources	*Soc1.* Whether their competitors have adopted, or are in the process of adopting, cyber security measures (Strongly agree – Strongly disagree) *Soc2.* Whether their customers believe they should adopt cyber security measures to protect their data (Strongly agree – Strongly disagree) *Soc3.* Whether companies they trade with believe they should adopt cyber security measures (Strongly agree – Strongly disagree) Questions derived from literature review
(3) Organizational Resources	*Org1.* Feeling that too much cyber security information is provided beyond my needs, resulting in perceptions of being overwhelmed (Strongly agree – Strongly disagree) *Org2.* I, sometimes, avoid looking for information about cyber security precautions even though I suspect I should (Strongly agree – Strongly disagree) *Org3.* SMEs cannot possibly follow ALL the advice (Strongly agree – Strongly disagree) *Org4.* There is so much advice online, and I am struggling to prioritize the recommended actions (Strongly agree – Strongly disagree) Adapted from (Cenfetelli and Schwarz, 2011; Plaks *et al.*, 2005; Igou, 2008)
(3) Personal Resources	*Pers1.* I can implement cyber security measures by myself (Strongly agree – Strongly disagree) *Pers2.* I personally know exactly what cyber security measures I should be implementing at work (Strongly agree – Strongly disagree) *Pers3.* Implementing cyber security measures is easy for me (Strongly agree – Strongly disagree) *Pers4.* I Have the capability to solve problems during the implementation of cyber security measures (Strongly agree – Strongly disagree) *Pers5.* I personally know exactly which cyber security measures I should be taking on my PERSONAL devices (Strongly agree – Strongly disagree) Adapted from (Chester and Beaudin, 1996)
Implementation of Cyber Controls and Precautions	*Ctrl1.* A tally of the rules or controls does the business has in place *Ctrl2.* A tally of aspects covered by their cyber security-related policies The controls we asked SMEs about in the survey were taken from (Department for Digital, Culture, Media and Sport, 2019)
Demographics	Size; Region; Sector; Owner/Employee; Remote working and policies; Use of online services

Table 3. Constructs and questions to measure them. (Number in parenthesis refers to Figure 1)

from one-person businesses. A total of 167 respondents (46.26%) were business owners, while 190 respondents (52.63%) were employees. A couple of respondents indicated that they were self-employed but not the business owner or else a partner in the business.

The majority of respondents indicated England as their primary business region (85.6%). The most represented industry sectors included: Education (11.4%); Professional, scientific or technical activities, including accountants (10.0%); and Retail trade (8.6%). Overall, more than 24 different industry sectors were represented.

About a quarter of respondents (26.6%) have business premises but also work remotely. This is particularly the case for one-person businesses, which represent almost half of this total. Remote working introduces additional vulnerabilities that require managing cyber security and data privacy risks. However, only 13.6% of respondents have additional rules in place for the remote working situation to ensure that cyber security is maintained.

Most businesses have accounts or pages on social media sites such as Facebook or Twitter (59.6%) and use an online business bank account (59.8%). Other online activity includes the ability for customers to buy products (37.4%) and for customers to access services (46.3%). Overall, 345 (95.6%) businesses engaged in some form of online activity. As such this allows them to conduct business with people outside their own geographical area while, at the same time, increasing their vulnerability to online threats.

Referring back to the numbering in Figure 1, we now report on each of the aspects raised during the literature review:

(1) Importance of cyber security to business continuity

To confirm the reality of the cyber threat, as well as our participants' experiences of being attacked, we asked respondents whether any cyberattacks happened to their business in the last year. The majority of incidents fell into one of seven categories (Figure 3).

Phishing is clearly a primary threat to these small businesses. When analyzing the most experienced attack (i.e. receiving fraudulent emails or being directed to fraudulent websites) according to business size, we observe that all businesses are at risk, with single-person businesses reporting the highest percentage (32.38%) of attacks.

When asked about the consequences of attacks that were experienced, the following were most commonly reported: (1) being unable to work due to loss of access to data (22%), (2) websites or online services being taken down (19%) and (3) software or systems being corrupted or damaged (15%). Other reported issues include time spent running malware and

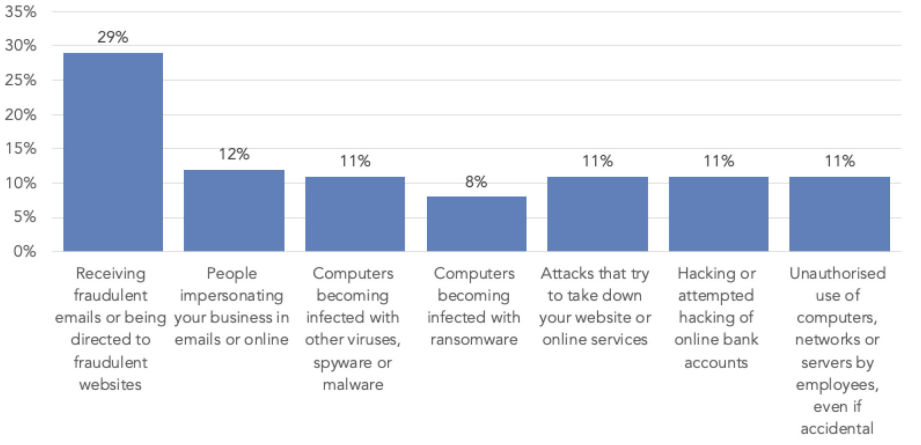


Figure 3.
Attacks experienced by SMEs

antivirus software and loss of emails. One business reported that consequences of an attack were still being assessed. Of the businesses that experienced an attack, all reported some form of negative consequence(s).

As expected and depicted in Figures 4 and 5, 80.9% of the respondents rated cyber security as a very or fairly high priority. A greater percentage of single-person (28%) and micro (24.3%) businesses rated cyber security as a low priority. Priority was not influenced by business region or industry sector. Hence, this particular factor does not appear to be triggering low situational awareness.

(2) Awareness

(2a) Awareness of threats

When asked if and where participants had searched for information, advice or guidance on cyber security over the last year, 184 (51%) of respondents reported not seeking anything. The rest found information by searching online (24.4% of cases). Only 4.2% searched for advice from Government websites, with 3.6% consulting software suppliers and 3.9% security companies.

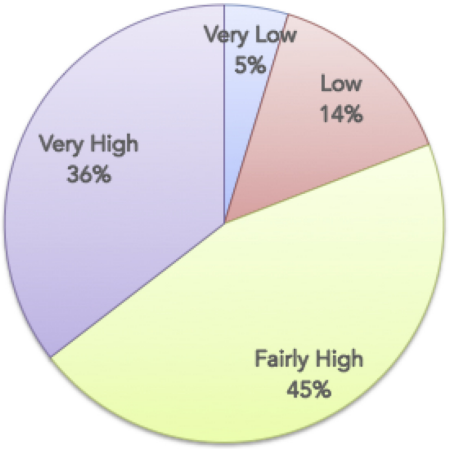


Figure 4.
Imp1: Self-reported priority of cyber security for SMEs

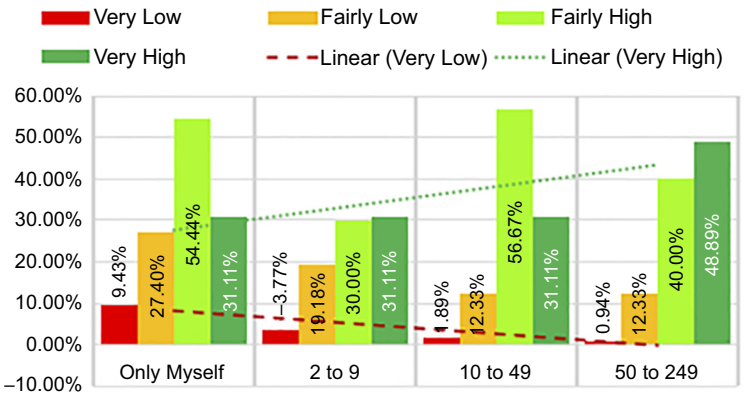


Figure 5.
Imp1: Self-reported Cyber security priority according to business size

When asked specifically about the usefulness of cyber security information, advice or guidance from Government, 57.3% of respondents rated this as very or fairly useful, with 20% not realizing that the Government was offering any cyber security advice. There is a significant correlation ($p < 0.01$) between business size and self-reported usefulness of Government guidance. A greater percentage of medium businesses (70%) find Government guidance very or fairly useful, as compared to small (65.6%), micro (56.7%) and single-person (40.2%) businesses. Indeed, 35.5% of single-person businesses are not aware of any Government advice on cyber security. This high percentage is concerning.

(2b) Awareness of precautions and controls

The number of respondents reporting to know about various Government schemes, which assist them in knowing about precautions and controls included: Cyber Aware campaign (113–31%); Small Business Guides (105–29%); Cyber Essentials (91–25%); and The ten Steps to Cyber Security (87–24%). For most, knowledge about a scheme is more common as business size increases.

About 56% of participants agreed with the statement: "*Too much cyber security information is provided beyond my needs, resulting in perceptions of being overwhelmed.*" and 47% agreed with: "*I sometimes avoid looking for information about cyber security precautions even though I suspect I should.*" Finally, 55% agreed that "*SMEs cannot possibly follow ALL the advice.*" Hence, many of our participants feel overwhelmed by the amount of advice and avoid looking for advice.

(2c) Awareness of need to act

Some SMEs suffer from the "halo effect" (Figure 6) and so do not take any action. There are also those who feel that they are too insignificant to attack (Figure 7). These two categories of SMEs are likely not to act in terms of implementing controls and taking precautions.

We asked participants whether they agreed that "Employees help each other to spot Phishing messages." About 243 SMEs responded to this question, with 79.8% agreeing. However, only 24 answered the following question in the affirmative: "*assigning employees general responsibility for cyber security*" and only 21 said that they had "*employee(s) whose job role includes cyber security or governance.*" It seems as if SMEs and their employees still believe that cyber security is a solo activity.

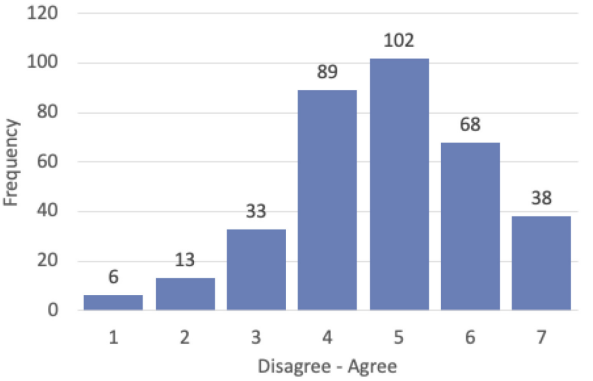
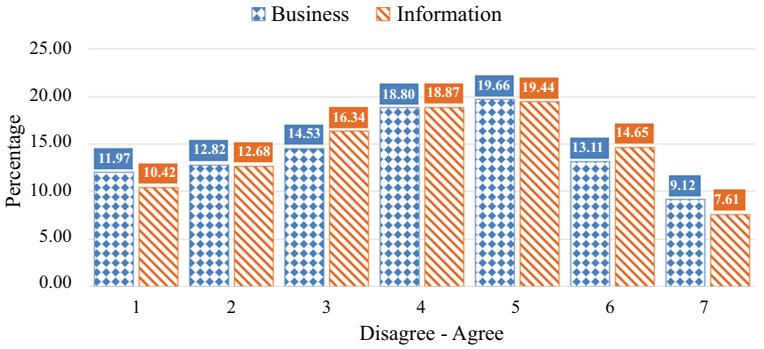


Figure 6.
Halo effect

Note(s): I haven't been attacked so what I'm doing must be good enough
1 = Disagree; 7 = Agree

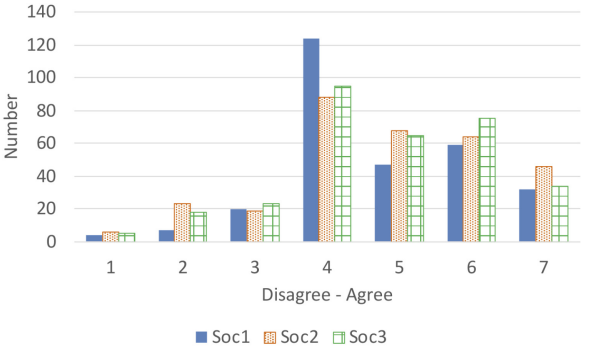


Note(s): *Business*: My business is too small for hackers to bother with me.
Information: I don't have any information that hackers would be interested in

Figure 7.
Insignificance

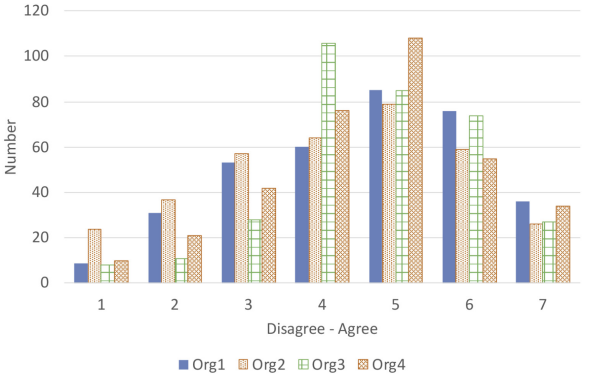
(3) Resources

Figure 8 shows whether participant SMEs perceive pressure from others, which makes up their social resources. Figure 9 shows the organizational resources of participant SMEs, and Figure 10 demonstrates the personal resources of participant SMEs.



Note(s): X Axis labels refer to Table 3

Figure 8.
Social resources



Note(s): X Axis labels refer to Table 3

Figure 9.
Organizational resources

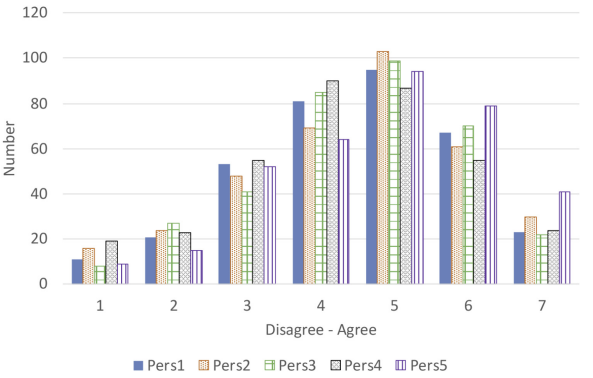


Figure 10.
Personal resources

Note(s): X Axis labels refer to Table 3

4.2 Implementation of controls and precautions

Some SMEs had password policies and we asked those SMEs to give us three pieces of advice about "good password requirements." We then rated the advice as correct (aligned with best practice), incorrect (not aligned) or irrelevant (e.g. just the word "Strong" without any explanation), using the most recent best practice advice to judge correctness (Prior and Renaud, 2020). About 274 respondents offered no guidelines, 5 gave one guideline, 32 gave two guidelines and 52 gave three guidelines. Of those who provided advice, 17 gave advice that could not be interpreted, e.g. "yes" or "none." Two of the most common misperceptions were related to the need for passwords to be complex (54 = 60%), and for passwords to expire (29 = 32%), with 23 (25%) citing both as best practice guidelines. Both of these mandates are outdated and lead to weaker passwords. As can be seen from Figure 11, only one person gave three pieces of correct advice, with 18 (20%) giving one correct guideline in response to this question and 6 (7%) giving two correct guidelines.

Businesses reportedly had a number of risk management arrangements in place (Figure 12). Only 85 (23.5%) of businesses implemented one or more arrangements, and 78 (21.6%) either do not know or have not got any of these arrangements in place.

Cyber security-related policies can cover various aspects, with the most frequently reported ones being: (1) remote or mobile working (32%); (2) employee permissions on business IT devices (32%); and (3) what can be stored on removable devices (31%). Examining policies, it was seen that 147 (40.7%) of businesses reported not covering any of these aspects or not having any cyber security-related policies.

Respondents reported taking a number of actions in the last year to identify cyber security risks to their business (Figure 13). Other actions reported include using penetration testing

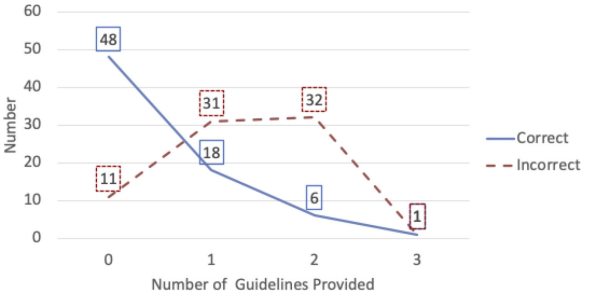


Figure 11.
SMEs' password "best practice" correct/ incorrect advice

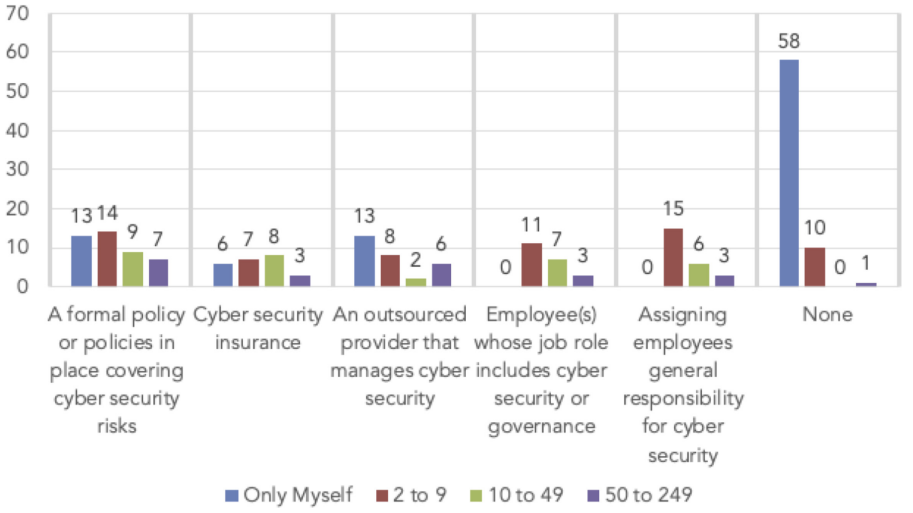


Figure 12.
Imp2: % of SMEs implementing Risk Management arrangements implemented

services (e.g. Shodan), installing security suites, weekly system updates and reading blogs. About 64 (17.7%) of respondents reported not taking any of these steps to identify cyber security risks.

4.2.1 Deployed cyber security controls. The number of SMEs who have rules and controls in place is shown in Figure 14. Only 28 (7.8%) respondents reported not having any of the listed rules or controls in place. The average number of rules and controls in place was 4.54, with 58.9% of businesses having at least four rules or controls in place. A total of 76.2% of respondents reported that they regularly run security software to remove malware from computers.

We also found that the bigger the business, the more controls that were implemented. However, there was no link between business size and the number of cyber security incidents reported.

4.3 Model validation

To test our model, an analysis using partial least squares structural equation modeling (PLS-SEM) was performed. PLS-SEM is an ordinary least squares regression-based method to

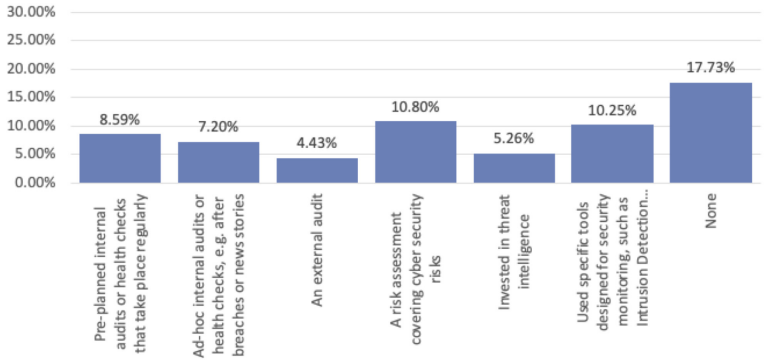


Figure 13.
Imp2: Number of risk identification measures

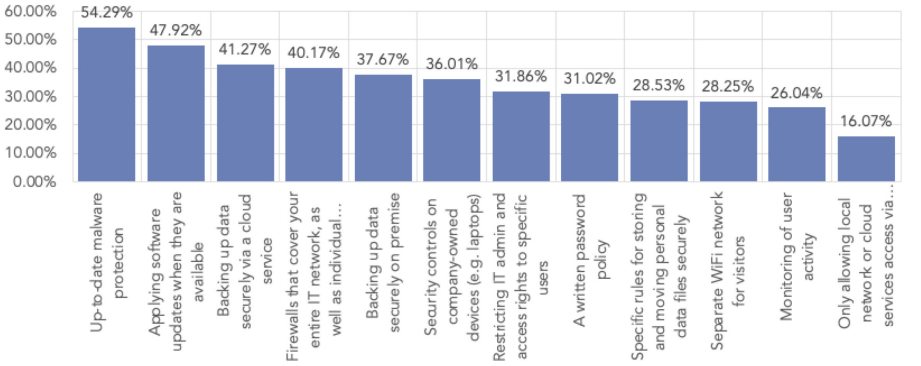


Figure 14.
Ctrl1: Implemented rules and controls

estimate the path relationships in the model. This approach is suitable for validating predictive models, particularly when the path model includes formatively measured constructs (Hair *et al.*, 2019). In our model, this is the case for the Cyber Situational Awareness construct. The SmartPLS (Ringle *et al.*, 2015) software tool (version 3.3.3) was used for analysis.

4.3.1 Analysis of the measurement model. The model proposed in this study consists of both reflective and formative constructs. "Importance of Cyber Security", "Social Resources", "Organizational Resources", "Personal Resources" and "Implementation of Cyber Controls and Precautions" are reflective constructs. "Cyber Situational Awareness" is a formative construct.

To assess the reflective constructs, we first examined indicator loadings. As Table 4 indicates, all but two values were above the recommended 0.708 threshold. After relevance testing (Hair *et al.*, 2016), the two indicators that were slightly below the threshold (Imp3 and

		Convergent validity			Internal consistency reliability		
Latent var	Indicators	Loadings	Indicator reliability	AVE	Composite reliability	Cronbach's alpha	Discriminant validity
Importance of Cyber Security	Imp1	0.816	0.666	0.557	0.789	0.684	Yes
	Imp2	0.719	0.517				
	Imp3	0.698	0.487				
Soc Resources	Soc1	0.735	0.540	0.631	0.836	0.713	Yes
	Soc2	0.869	0.755				
	Soc3	0.773	0.598				
Org Resources	Org1	0.774	0.599	0.573	0.843	0.757	Yes
	Org2	0.816	0.666				
	Org3	0.722	0.521				
	Org4	0.711	0.506				
Personal Resources	Pers1	0.612	0.375	0.621	0.890	0.856	Yes
	Pers2	0.849	0.721				
	Pers3	0.808	0.653				
	Pers4	0.816	0.666				
	Pers5	0.833	0.694				
Impl of Cyber Controls and Precautions	Ctrl1	0.915	0.837	0.844	0.915	0.815	Yes
	Ctrl2	0.922	0.850				

Table 4.
Results summary for reflective measurement model

Pers1) were retained. Next, internal consistency reliability was assessed using composite reliability (for completeness Cronbach's alpha is reported in Table 4 as well). All composite reliability values were satisfactory (above 0.70) with no problematic values above 0.95 (Diamantopoulos *et al.*, 2012). Evaluating the convergent validity of each construct measure indicates that the average variance extracted (AVE) is above an acceptable value of 0.50. Lastly, discriminant validity was assessed using the heterotrait–monotrait (HTMT) ratio of correlations. All values were below the conservative threshold value of 0.85 (Henseler *et al.*, 2015), as indicated in Table 5. A bootstrap confidence interval was derived (using 5,000 samples) with no confidence interval including the value 1, thus confirming discriminant validity.

We conceptualized "Cyber Situational Awareness" as a formative construct with four indicators. These relate to the three dimensions captured in this construct, namely the awareness of cyber security threats, precautions and the need to act. We assessed indicator collinearity using the variance inflation factor (VIF). There were no indicators with critical levels of collinearity (i.e. VIF $\geq$ 5 (Hair *et al.*, 2016)), with values ranging from 1.029 to 1.263.

Next, we analyzed the outer weights for their significance and relevance, using a bootstrapping procedure with 5,000 samples. The result of this analysis is summarized in Table 6. All indicator outer weights were significant and therefore retained. Considering that all reflective and the formative constructs exhibit satisfactory levels of quality, we thus proceeded with the evaluation of the structural model.

4.3.2 Analysis of the structural model. We started the evaluation of the structural model by looking for collinearity issues. We examined the VIF values of all sets of predictor constructs in the structural model. Since all VIF values were below the threshold of 5 (ranging from 1.031 to 1.091), collinearity among the predictor constructs is not an issue in the structural model.

Evaluating the coefficient of determination (R^2 value) indicated a value of 0.230 for "Cyber Situational Awareness" and 0.363 for "Implementation of Cyber Controls and Precautions" (respectively explaining 23 and 36.3% of variance). Examining the f^2 effect size, we observe that "Importance of Cyber Security" has a medium effect size of 0.166 on "Cyber Situational Awareness." In addition, "Cyber Situational Awareness" has a large effect size of 0.340 on

	Ctrl	Imp	Org	Pers	Soc
(Ctrl) Implementation of Cyber Controls and Precautions					
(Imp) Importance of Cyber Security	0.481				
(Org) Organizational Resources	0.365	0.197			
(Pers) Personal Resources	0.262	0.381	0.080		
(Soc) Social Resources	0.452	0.345	0.152	0.543	

Table 5. Heterotrait–monotrait ratio of correlations

Formative construct	Formative indicators	Outer weights	*t* value	*p* value	95% BCa confidence interval	Significance ($p < 0.05$)?
Cyber Situational Awareness	CSA1	0.332	4.015	0.000	[0.171, 0.493]	Yes
	CSA2	0.443	4.409	0.000	[0.252, 0.640]	Yes
	CSA3	−0.279	2.915	0.004	[−0.473, −0.095]	Yes
	CSA4	0.555	6.585	0.000	[0.388, 0.712]	Yes

Table 6. Results summary for formative construct significance testing

"Implementation of Cyber Controls and Precautions." All other f^2 values showed small effects, ranging from 0.031 to 0.066. We also analyzed the path model's predictive accuracy by calculating the Q^2 value using the cross-validated redundancy approach (Hair *et al.*, 2016). The reflective endogenous construct "Implementation of Cyber Controls and Precautions" has a Q^2 value of 0.295 that indicates medium predictive relevance of the model.

To analyze the significance of relationships, we used a bootstrapping procedure with 5,000 samples. Assuming a 5% significance level, we find that all relationships in the structural model are significant (in fact, all were significant at $p < 0.001$). The results are summarized in Table 7, while Figure 15 shows the final validated SME Cyber Situational Awareness model. The model indicates the coefficient of determination for the endogenous constructs and path coefficients for all the hypothesized relationships.

5. Discussion and conclusion

Our aim with this study was to examine how SMEs' cyber situational awareness influences the implementation of cyber security controls and precautions. We used Endsley's model of situational awareness as a lens, deriving a number of factors from the literature that can be expected to influence SMEs' cyber situational awareness and also factors that influence the implementation of controls and precautions within SMEs. Here, we discuss the implications for research and practice and also present the limitations of our study.

Table 7.
Significance testing results of the structural model path coefficients

Hypothesis	Path coefficients	t values	p values	95% confidence intervals	Significance ($p < 0.05$)?
H1	0.374	9.429	0.000	[0.287, 0.443]	Yes
H2	0.210	4.249	0.000	[0.103, 0.297]	Yes
H3	0.208	5.215	0.000	[0.126, 0.281]	Yes
H4	0.143	3.490	0.000	[0.062, 0.221]	Yes
H5	0.483	13.633	0.000	[0.401, 0.545]	Yes

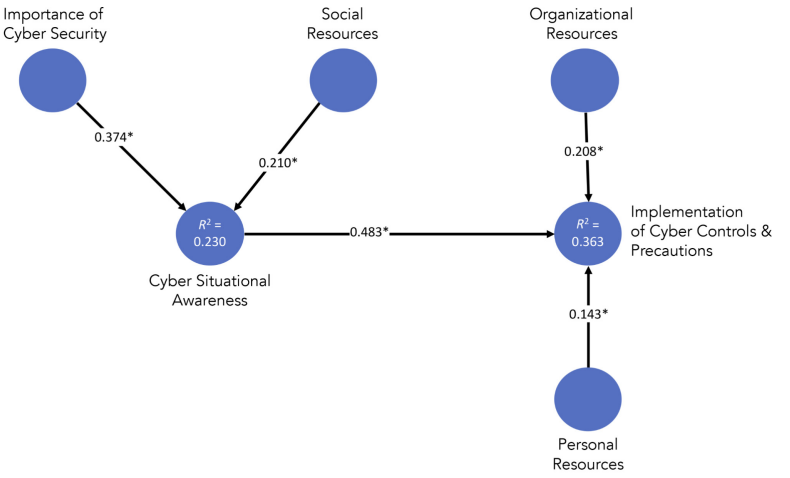


Figure 15.
Results of the PLS–SEM analysis

Note(s): *Significant at $p < 0.001$

5.1 Implications for research

The results of our analysis highlight the influence of understanding the importance of cyber security, followed by the availability of resources. With respect to cyber situational awareness and understanding the importance of cyber security, SMEs need trusted and *actionable cyber security advice*, tailored to their context. In the UK, this is available from Government advice sources on the Web. We do not know why these business owners and employees preferred to use general online searches to obtain advice. It could be a simple matter of a lack of awareness. If this is the case, it can be addressed by advertising campaigns and by disseminating the information via small business federations and chambers of commerce. Efforts should be directed at making businesses aware of official cyber security schemes and enabling them to participate.

An alternative explanation is that there is a general lack of trust in the government, in our case the UK. There is evidence of this phenomenon (Williams *et al.*, 2020), and it seems that such trust has been compromised during the pandemic of 2020 (Sibley *et al.*, 2020), during which we collected our data. If this is behind the low usage of government advice, it is much harder to address. The issue of trust in cyber security advice sources is an important topic for further research.

The predictive relevance of the situational awareness theory in modeling cyber security behaviors has been demonstrated in this study. This supports previous research arguing for the applicability of this theory in cyber security (Franke and Brynielsson, 2014), offering an alternative to theories (e.g. Protection Motivation Theory) that have been used extensively in the cyber domain. However, research should focus on developing and validating additional measures for cyber situational awareness, focusing on each of the three levels (Endsley, 1985, 1995). In this way, a more fine-grained analysis of the construct may be possible.

5.2 Implications for practice

Our analysis suggests several interventions to remove the barriers we have identified. With respect to organizational resources, SMEs need to *re-align outdated password practices*. Passwords are a fundamental aspect of system security but needs to be aligned with best practice to remain effective. Adopting outdated practices presents a security risk and could place undue cognitive burden on the user. Password best practice is provided by the NCSC in the UK [4] but might need to be disseminated in the form of an infographic to engage users.

With respect to personal resources, SMEs' *misperceptions need to be addressed*. In particular, just because they have not yet been attacked does not mean that (1) their current practice is sufficient or (2) they are too insignificant to be attacked [the opposite is the case (Zurich, 2020)]. They should be made aware of the fact that there is often a lag between when a breach occurs and when it is detected, which means that no one can really be sure that they have not experienced an attack (Vargas, 2019). Remaining alert and focusing on continuous improvement of security processes will ensure business resilience.

With respect to social resources, SMEs should be advised that *local "Cyber Champions" can contribute* towards strengthening their cyber security. This is a mindset change in a field where many consider cyber security to be a solo game. However, there are indications from other domains that ensuring that all employees feel responsible for cyber security and that they support each other could contribute to better business cyber security (Zimmermann and Renaud, 2019).

5.3 Limitations and future work

Our findings are based on empirical data about SMEs in the UK, which provides scope for comparison studies in other countries. We would assume that situational conditions are also

influential and thus our results – based on data collected in the UK during the 2020 pandemic – should be interpreted against this backdrop.

The model proposed in Figure 2 is not comprehensive, nor is it intended to reflect all possible influences on cyber situational awareness. We have used an Occam's razor approach to propose a first model, which we hope other researchers will extend with newly identified factors to build towards a more comprehensive model, over time.

Notes

1. https://www.fsb.org.uk/
2. https://www.oscr.org.uk/news/cyber-essentials-grants/
3. https://www.statista.com/statistics/586565/cyber-essentials-scheme-awareness-by-united-kingdom-uk-businesses/
4. https://www.ncsc.gov.uk/collection/passwords

References

Almeida, F., Carvalho, I. and Cruz, F. (2018), "Structure and challenges of a security policy on small and medium enterprises", *KSII Transactions on Internet and Information Systems*, Vol. 12 No. 2, pp. 747-763.

Barlette, Y. and Jaouen, A. (2019), "Information security in SMEs: determinants of CEOs' protective and supportive behaviors", *Systemes d'Information Management*, Vol. 24 No. 3, pp. 7-40.

Barlette, Y., Gundolf, K. and Jaouen, A. (2017), "CEOs' information security behavior in SMEs: does ownership matter?", *Systemes d'Information Management*, Vol. 22 No. 3, pp. 7-45.

Bell, S. (2017), "Cybersecurity is not just a 'big business' issue", *Governance Directions*, Vol. 69 No. 9, p. 536.

Berry, C. and Berry, R. (2018), "An initial assessment of small business risk management approaches for cyber security threats", *International Journal of Business Continuity and Risk Management*, Vol. 8 No. 1, pp. 1-10.

Brodin, M. and Rose, J. (2020), "Improving mobile security management in SME's: the MSME framework", *Journal of Information System Security*, Vol. 16 No. 1, pp. 47-75.

BullGuard (2020), "New study reveals one in three SMBs use free consumer cybersecurity and one in five use no endpoint security at all", available at: https://www.prweb.com/releases/new_study_reveals_one_in_three_smbs_use_free_consumer_cybersecurity_and_one_in_five_use_no_endpoint_security_at_all/prweb16921507.htm.

Cenfetelli, R.T. and Schwarz, A. (2011), "Identifying and testing the inhibitors of technology usage intentions", *Information Systems Research*, Vol. 22 No. 4, pp. 808-823.

Chester, M.D. and Beaudin, B.Q. (1996), "Efficacy beliefs of newly hired teachers in urban schools", *American Educational Research Journal*, Vol. 33 No. 1, pp. 233-257.

Cholez, H. and Girard, F. (2014), "Maturity assessment and process improvement for information security management in small and medium enterprises", *Journal of Software: Evolution and Process*, Vol. 26 No. 5, pp. 496-503.

Chung, M. (2020), "Signs your cyber security is doomed to fail", *Computer Fraud and Security*, Vol. 2020 No. 3, pp. 10-13.

CsC, P.H. and Stehílková, B. (2011), "Information security management in small and medium enterprises", *International Multidisciplinary Scientific Geo Conference: SGEM: Surveying Geology & Mining Ecology Management*, Surveying Geology & Mining Ecology Management (SGEM), Vol. 2, p. 527.

CyberAware (2021), "6 ways to improve your online security", available at: https://www.ncsc.gov.uk/cyberaware/home (accessed 4 March 2021).

CyberEssentials (2021), "About cyber essentials", available at: https://www.ncsc.gov.uk/cyberessentials/overview (accessed 4 March 2021).

Department for Digital, Culture, Media & Sport (2019), "Cyber security breaches survey 2019", available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020 (accessed 27 December 2020).

Department for Digital, Culture, Media & Sport (2021), "Cyber security breaches survey 2021", available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021 (accessed 15 June 2021).

Diamantopoulos, A., Sarstedt, M., Fuchs, C., Wilczynski, P. and Kaiser, S. (2012), "Guidelines for choosing between multi-item and single-item scales for construct measurement: a predictive validity perspective", *Journal of the Academy of Marketing Science*, Vol. 40 No. 3, pp. 434-449, 00984.

Endsley, M.R. (1985), "Toward a theory of situation awareness in dynamic systems", *Human Factors*, Vol. 37 No. 1, pp. 32-65.

Endsley, M.R. (1995), "A taxonomy of situation awareness errors", *Human Factors in Aviation Operations*, Vol. 3 No. 2, pp. 287-292.

ENISA (2015), "Information security and privacy standards for SMEs", available at: www.enisa.europa.eu (accessed 3 March 2021).

Franke, U. and Brynielsson, J. (2014), "Cyber situational awareness – a systematic review of the literature", *Computers and Security*, Vol. 46, pp. 18-31.

Gafni, R. and Pavel, T. (2019), "The invisible hole of information on SMB's cybersecurity", *Online Journal of Applied Knowledge Management (OJAKM)*, Vol. 7 No. 1, pp. 14-26.

González, D.P., González, P.S. and Preciado, S.T. (2013), "Strategy of information security in small and medium enterprises, an technology-enterprise approach: analysis of its relationship with organizational and performance business variables", *Information (Japan)*, Vol. 16 No. 6, pp. 3883-3905.

Gundu, T. (2019), "Acknowledging and reducing the knowing and doing gap in employee cybersecurity complaince", *ICCWS 2019 14th International Conference on Cyber Warfare and Security*, pp. 94-102.

Hair, J.F., Hult, G.T.M., Ringle, C.M. and Sarstedt, M. (2016), *A Primer on Partial Least Squares Structural Equation Modeling*, 2nd ed., SAGE Publications, Los Angeles.

Hair, J.F., Risher, J.J., Sarstedt, M. and Ringle, C.M. (2019), "When to use and how to report the results of PLS-SEM", *European Business Review*, Vol. 31 No. 1, pp. 2-24.

Harris, M.A. and Patten, K.P. (2014), "Mobile device security considerations for small- and medium-sized enterprise business mobility", *Information Management and Computer Security*, Emerald Group Publishing, Bradford, Vol. 22 No. 1, pp. 97-114, available at: https://search.proquest.com/docview/1505350532?accountid=14500.

Heidt, M., Gerlach, J. and Buxmann, P. (2019), "Investigating the security divide between SME and large companies: how SME characteristics influence organizational IT security investments", *Information Systems Frontiers*, Vol. 21 No. 6, pp. 1285-1305.

Henseler, J., Ringle, C.M. and Sarstedt, M. (2015), "A new criterion for assessing discriminant validity in variance-based structural equation modeling", *Journal of the Academy of Marketing Science*, Vol. 43 No. 1, pp. 115-135.

Hutchings, A., Smith, R. and James, L. (2013), "Cloud computing for small business: criminal and security threats and prevention measures", *Trends and Issues in Crime and Criminal Justice*, Vol. May No. 456, pp. 1-8.

Ifinedo, P. (2012), "Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory", *Computers and Security*, Vol. 31 No. 1, pp. 83-95.

Igou, E.R. (2008), "'How long will I suffer?' versus 'How long will you suffer?' A self-other effect in affective forecasting", *Journal of Personality and Social Psychology*, Vol. 95 No. 4, pp. 899-917.

Imsand, E., Tucker, B., Paxton, J. and Graves, S. (2019), "A survey of cyber security practices in small businesses", *National Cyber Summit*, Springer, Cham, pp. 44-50.

Kabanda, S., Tanner, M. and Kent, C. (2018), "Exploring SME cybersecurity practices in developing countries", *Journal of Organizational Computing and Electronic Commerce*, Vol. 28 No. 3, pp. 269-282.

Kaušpadienė, L., Ramanauskaitė, S. and Čenys, A. (2019), "Information security management framework suitability estimation for small and medium enterprise", *Technological and Economic Development of Economy*, Vol. 25 No. 5, pp. 979-997.

Kent, C., Tanner, M. and Kabanda, S. (2016), "How South African SMEs address cyber security: the case of web server logs and intrusion detection", *IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, IEEE, pp. 100-105.

Kimwele, M., Mwangi, W. and Kimani, S. (2010), "Adoption of information technology security policies: case study of Kenyan small and medium enterprises (SMEs)", *Journal of Theoretical and Applied Information Technology*, Vol. 18 No. 2, pp. 1-11.

Kurpjuhn, T. (2015), "The SME security challenge", *Computer Fraud and Security*, Vol. 2015 No. 3, pp. 5-7.

Lacey, D. and James, B.E. (2010), "Review of availability of advice on security for small/medium sized organisations", available at: https://ico.org.uk/media/1042344/review-availablility-of-security-advice-for-sme.pdf (accessed 6 June 2021).

Lee, Y.-J., Choi, S.-S. and Yeon, K.-J. (2019), "An analysis on the web security threats of small & medium enterprise through web vulnerability inspection", *International Journal of Advanced Science and Technology*, NADIA, Vol. 129, pp. 171-182, doi: 10.33832/ijast.2019.129.15.

Lejaka, T.K., Da Veiga, A. and Loock, M. (2019), "Cyber security awareness for small, medium and micro enterprises (SMMEs) in South Africa", *Conference on Information Communications Technology and Society (ICTAS)*, IEEE, pp. 1-6.

Lent, R.W., Hoffman, M.A., Hill, C.E., Treistman, D., Mount, M. and Singley, D. (2006), "Client-specific counselor self-efficacy in novice counselors: relation to perceptions of session quality", *Journal of Counseling Psychology*, Vol. 53 No. 4, pp. 453-463.

Lewis, S. (2020), "Cyber attack warning for SMEs as risks heighten amid covid-19 pandemic". available at: https://www.professionaljeweller.com/cyber-attack-warning-for-smes-as-risks-heighten-amid-covid-19-pandemic/ (accessed 27 December 2020).

Lloyd, G. (2020), "The business benefits of cyber security for SMEs", *Computer Fraud and Security*, Vol. 2020 No. 2, pp. 14-17.

Manheim, L. (2014), "Information non-seeking behaviour", *Proceedings of ISIC: the Information Behaviour Conference*, Vol. Part 1.

Marett, K. and Barnett, T. (2019), "Information security practices in small-to-medium sized businesses: a hotspot analysis", *Information Resources Management Journal*, Vol. 32 No. 2, pp. 76-93.

Mitrofan, A.L., Cruceru, E.V. and Barbu, A. (2020), "Determining the main causes that lead to cybersecurity risks in SMEs", *Business Excellence and Management*, Vol. 10 No. 4, pp. 38-48.

Muncaster, P. (2020), "Over 50,000 UK SMEs could collapse following cyber-attack", available at: https://www.infosecurity-magazine.com/news/over-50000-uk-smes-could-collapse/ (accessed 28 December 2020).

Nachreiner, C. (2012), "Size isn't everything: why cyber attackers target SMEs", available at: https://www.secplicity.org/2012/12/03/size-isnt-everything-why-cyber-attackers-target-smes/.

Ncubukezi, T., Mwansa, L. and Rocaries, F. (2020), "A review of the current cyber hygiene in small and medium-sized businesses", *2020 15th International Conference for Internet Technology and Secured Transactions (ICITST)*, IEEE, pp. 1-6.

Njenga, K. and Jordaan, P. (2016), "We want to do it our way: the neutralisation approach to managing information systems security by small businesses", *The African Journal of Information Systems*, Vol. 8 No. 1, pp. 42-63.

Noguerol, L.O. and Branch, R. (2018), "Leadership and electronic data security within small businesses: an exploratory case study", *Journal of Economic Development, Management, IT, Finance, and Marketing*, Global Strategic Management, Beverly Hills, Vol. 10 No. 2, pp. 7-35.

Pagura, I. (2020), "Law report: small business and cyber security", *Journal of the Australian Traditional-Medicine*, Vol. 26 No. 1, pp. 38-39, available at: https://search.informit.com.au/documentSummary;dn=070004091643509;res=IELHEA.

Patterson, J. (2017), "Cyber-security policy decisions in small businesses", PhD thesis, College of Management and Technology.

Perez, C. (2020), "A cybersecurity strategy for the small business", Master's thesis, Cybersecurity, Utica College.

Persoskie, A., Ferrer, R.A. and Klein, W.M. (2014), "Association of cancer worry and perceived risk with doctor avoidance: an analysis of information avoidance in a nationally representative us sample", *Journal of Behavioral Medicine*, Vol. 37 No. 5, pp. 977-987.

Plaks, J.E., Grant, H. and Dweck, C.S. (2005), "Violations of implicit theories and the sense of prediction and control: implications for motivated person perception", *Journal of Personality and Social Psychology*, Vol. 88 No. 2, pp. 245-262.

Prior, S. and Renaud, K. (2020), "Age-appropriate password 'best practice' ontologies for early educators and parents", *International Journal of Child-Computer Interaction*, Vol. 23, pp. 100169-100224, doi: 10.1016/j.ijcci.2020.100169.

Redmiles, E.M., Warford, N., Jayanti, A., Koneru, A., Kross, S., Morales, M., Stevens, R. and Mazurek, M.L. (2020), "A comprehensive quality evaluation of security and privacy advice on the web", *29th USENIX Security Symposium USENIX Security 20*, pp. 89-108.

Renaud, K. and Dupuis, M. (2019), "Cyber security fear appeals: unexpectedly complicated", *Proceedings of the New Security Paradigms Workshop*, pp. 42-56.

Renaud, K. and Weir, G.R. (2016), "Cybersecurity and the unbearability of uncertainty", *2016 Cybersecurity and Cyberforensics Conference (CCC)*, IEEE, pp. 137-143.

Reuter, C. (2015), "Towards efficient security: business continuity management in small and medium enterprises", *International Journal of Information Systems for Crisis Response and Management*, Vol. 7 No. 3 July 2015, pp. 69-79, doi: 10.4018/IJISCRAM.2015070105.

Ringle, C.M., Wende, S. and Becker, J.-M. (2015), "Smartpls 3", available at: http://www.smartpls.com.

Robert Johnson, I. (2019), "60 percent of small companies close within 6 Months of being hacked", available at: https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/ (accessed 6 June 2021).

Sangani, N.K. and Vijayakumar, B. (2012), "Cyber security scenarios and control for small and medium enterprises", *Informatica Economica*, INFOREC Association, Bucharest, Vol. 16 No. 2, pp. 58-71.

Sangster, M. (2020), "When it comes to cyber security, ignorance isn't bliss–it's negligence", *Network Security*, Vol. 2020 No. 12, pp. 8-12.

Schneider, K.N. (2013), "Improving data security in small businesses", *Journal of Technology Research*, Academic and Business Research Institute, Vol. 4, p. 1.

Sharma, K., Singh, A. and Sharma, V.P. (2009), "SMEs and cybersecurity threats in e-commerce", *EDPACS The EDP Audit, Control, and Security Newsletter*, Vol. 39 Nos 5-6, pp. 1-49.

Shred-it (2011), "Small businesses underestimate impact of data security", *International Journal of Micrographics and Optical Technology*, Research Information, Burnham, Vol. 29 Nos 4/5, p. 8.

Sibley, C.G., Greaves, L.M., Satherley, N., Wilson, M.S., Overall, N.C., Lee, C.H., Milojev, P., Bulbulia, J., Osborne, D., Milfont, T.L. and Houkamau, C.A. (2020), "Effects of the covid-19 pandemic and nationwide lockdown on trust, attitudes toward government, and well-being", *American Psychologist*, Vol. 75 No. 5, p. 618.

SMESEC (2021), "Cybersecurity for small and medium-sized enterprises (SMESEC) a lightweight cybersecurity framework for thorough protection", available at: https://www.smesec.eu/index.html.

Todd, M. and Rahman, S. (2015), "Complete network security protection for SME's within limited resources", arXiv preprint arXiv:1512.00085 .

UK Department for Business, Energy & Industrial Strategy (n.d.), "Business population estimates 2020", available at: https://www.gov.uk/government/statistics/business-population-estimates-2020 (accessed 3 March 2021).

Vance, A., Siponen, M. and Pahnila, S. (2012), "Motivating is security compliance: insights from habit and protection motivation theory", *Information and Management*, Vol. 49 Nos 3-4, pp. 190-198.

Vargas, J. (2019), "The unacceptable time gap between a breach and its detection", available at: https://lumu.io/blog/the-unacceptable-time-gap-between-a-breach-and-its-detection/.

Ward, M. (2021), "Business statistics. briefing paper number 06152", available at: https://researchbriefings.files.parliament.uk/documents/SN06152/SN06152.pdf (accessed 4 March 2021).

Whitehead, G. (2020), "Investigation of factors influencing cybersecurity decision making in Irish SME's from a senior manager/owner perspective", PhD thesis, National College of Ireland, Dublin.

Williams, S.N., Armitage, C.J., Tampe, T. and Dienes, K. (2020), "Public perceptions and experiences of social distancing and social isolation during the COVID-19 pandemic: a UK-based focus group study", *BMJ Open*, Vol. 10 No. 7, p. e039334.

Williams, O. (2020), "Is the UK's cyber essentials scheme working?", available at: https://tech.newstatesman.com/security/cyber-essentials-scheme (accessed 27 December 2020).

Yigit Ozkan, B., Spruit, M., Wondolleck, R. and Burriel Coll, V. (2020), "Modelling adaptive information security for SMEs in a cluster", *Journal of Intellectual Capital*, Vol. 21 No. 2, pp. 235-256.

Zimmermann, V. and Renaud, K. (2019), "Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset", *International Journal of Human-Computer Studies*, Vol. 131, pp. 169-187.

Zurich (2020), "Cyber attacks – how vulnerable are SMEs?", available at: https://www.zurich.co.uk/news-and-insight/cyber-attacks-vulnerable-smes (accessed 5 March 2021).

About the authors

Karen Renaud is a Scottish computing Scientist at the University of Strathclyde in Glasgow, working on all aspects of Human-Centred Security and Privacy. She was educated at the Universities of Pretoria, South Africa and Glasgow. She is particularly interested in deploying behavioral science techniques to improve security behaviors, and in encouraging end user privacy-preserving behaviors. Karen Renaud is the corresponding author and can be contacted at: karen.renaud@strath.ac.uk

Jacques Ophoff is a Senior Lecturer in the Division of Cyber Security at Abertay University in the United Kingdom. He obtained his doctorate in Information Technology from the Nelson Mandela Metropolitan University, South Africa. His research interests include cyber security, privacy, digital forensics, mobile technologies, and education. He is a regular reviewer for international journals and Vice-Chair of IFIP WG 11.8: Information Security Education.